특 집

국제공통평가기준의 국내 현황과 국내·외 표준화 동향

이 태 승, 노 병 규
한국정보보호진흥원 평가기준팀

Ⅰ. 머리말

오늘날 세계는 정보통신기술의 발달로 인하여 정보통신시스템에 대한 의존도 및 활용도가 증가하고 있으며 네트워크간의 상호 연결을 통하여 전 세계를 하나로 잇는 정보화 사회가 형성되고 있다. 하지만 정보의 불법적 유출, 정보의 위 변조, 바이러스 피해 확산, 서비스 방해, 불건전 정보 유통, 해킹, 개인정보 침해 등 이른바 정보화 역기능 또한 확산되고 있어 이에 대한 보호대책의 필요성이 날로 증대되고 있다.

이러한 정보화 역기능의 위험으로부터 주요 자산을 보호하기 위한 제도적 노력의 일환으로 미국, 캐나다, 영국, 독일, 프랑스 등 선진국에서는 80년대부터 신뢰성이 입증된 정보보호시스템 공급을 위하여 정보보호시스템 평가 인증제도를 구축 운영하였다. 90년대 초부터 이들 국가들은 다양한 정보보호시스템 평가에 공통적으로 적용할 수 있는 단일화된 평가기준의 필요성에 따라 국제공통평가기준(CC, Common Criteria)을 개발·표준화하여 이를 정보보호시스템 평가 인증 등에 활용 중에 있다.

이에 본 고는 2002년부터 국내 평가·인증제도안으로 수용된 CC의 현황과 국내 표준기관 및 ISO/IEC JTC 1/SC 27을 중심으로 진행 중인 국내·외 표준화 동향을 소개함으로써, 국내 정보보호시스템 평가·인증 관계자가 CC를 효율적으로 활용하고 관련된 국제 동향을 파악하는 데 도움을 주고자 한다.

Ⅱ. CC의 국내 현황

1. 국내 평가·인증제도와 CC

국내 정보보호시스템 평가 인증제도는 정보화 촉진기본법 및 동법 시행령에 의거 1998년 2월 정보통신망 침입차단시스템 평가기준(정보통신부 고시 1998-19) 및 평가 지침서(정보통신부 고시 1998-20)가 고시되면서 시작되었다. 이후 개정된 침입차단시스템 평가기준(정보통신부 고시 2000-14)과 정보통신망 평가 인증지침(정보통신부 고시 2000-15)이 2000년 2월에 고시됨으로써 정보보호 산업체는 공공기관용과 민수용의 구분이 없는 단일 평가 인증체계 하에서 제품의 평가 인증 서비스를 받을 수 있게 되었다. 또한 국내 정보보호 시장의 침입탐지시스템 수요 증가에 따라 기존의 침입차단시스템에 이어 추가로 침입탐지시스템이 평가 인증 대상에 포함됨으로써(정보통신부 고시 2000-62, 정보통신부 고시 2001-24) 국내 정보보호산업이 정착할 수 있는 토대가 되었다.

2002년에는 다양한 제품평가 요구에 대한 신속한 대응과 국내 정보보호산업체의 국제 경쟁력을 강화하기 위하여 한국정보보호진흥원을 비롯한 국내 관계기관은 평가 인증제도의 국제적인 추세인 CC 버전 2.1을 국내 평가기준으로 수용한 정보보호시스템 공통평가기준(정보통신부 고시 2002-40)과 이를 시행하기 위한 정보보호시스템 평가 인증지침을 2002년 8월에 개정 고시(정보통신부 고시 2002-41)하였다.

이후 한국정보보호진흥원은 CC에 기반한 국가

기관용 침입차단시스템, 침입탐지시스템, 가상사설망 보호프로파일을 개발하여 2003년 현재 이들 제품군과 통합제품군을 대상으로 평가 중이며 다양한 제품군으로 평가대상을 확대 중에 있다.

2. CC의 개요

CC는 정보보호시스템에서 요구되는 일반적인 소개와 모델을 설명하는 1부와 기능 요구사항의 2부 그리고 보증요구사항 설명하는 3부로 구성되어 있으며 각 부에 관한 내용은 다음과 같다.

◦ 1부 : 소개 및 일반모델

정보보호시스템의 평가원칙과 일반개념을 정의하고 평가의 일반모델을 표현하는 CC를 소개하는 부분으로 정보보호시스템의 보안목적을 표현하고 보안요구사항을 정의하여 정보보호시스템의 상위 수준 명세를 작성하기 위한 구조를 소개하고 있다.

〈표 1〉 CC의 평가보증등급

보증클래스	보증패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상관리	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
배포 및 운영	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
개발	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
설명서	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
생명주기지원	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

◦ 2부 : 보안기능요구사항

평가대상의 보안기능을 표현하기 위한 기능컴포넌트들이 클래스, 패밀리, 컴포넌트의 계층관계로 구분되어 있으며 클래스 범주는 보안감사(FAU), 통신(FCO), 암호지원(FCS), 사용자 데이터보호(FDP), 식별·인증(FIA), 보안관리(FMT), 프라이버시(FPR), TSF 보호(FPT), 자원활용(FRU), TOE 접근(FTA), 안전한 경로·채널(FTP)의 총 11개를 포괄하고 있다.

◦ 3부 : 보증요구사항

보증 평가의 척도를 정의한 평가보증등급 EAL 1~EAL7과 보증등급을 구성하는 개별적인 보증 컴포넌트, 보호프로파일 및 보안목표명세서 평가를 위한 기준을 포함하고 있으며, 해당 컴포넌트는 보호프로파일 평가(APE), 보안목표명세서 평가(ASE), 형상관리(ACM), 배포 및 운영(ADO), 개발(ADV), 설명서(AGD), 생명주기 지원(ALC), 시험(ATE), 취약성평가(AVA)의 클래스로 분류되어 있다〈표 1 참조〉.

3. CC의 활용

위와 같이 구성된 CC는 기 평가기준의 조화를 통해 평가결과의 상호인정 기반마련, 국제적으로 표준화된 평가기준 적용, 중복평가로 인한 시간·비용 절감, 보안요구사항의 유연성 부여, 평가결과의 국제적 상호인정 등의 목적에 맞추어 아래와 같이 활용되고 있다.

◦ CC에 기반한 보호프로파일 개발·보급

CC에 기반한 평가가 2002년 8월에 시행되면서 침입차단시스템, 침입탐지시스템, 가상사설망 등 다양한 제품군에 대한 보호프로파일이 개발·보급되었으며, 현재 침입차단시스템 등 4개의 보호프로파일이 국가기관용으로 개발되어 등재되어 있다〈표 2 참조〉.

◦ CC 기반 제출물 작성 및 평가시행

CC를 기반으로 평가 중인 제품은 〈표 3〉과 같으며, 제품의 평가보증등급에서 요구하는 보안요구사항을 충족시키기 위하여, 제출물에는 보안목표명세서, 기능명세서, 기본설계서 사용자설명서, 생명주기지원서 등이 포함된다.

위의 CC 기반 보호프로파일 개발·보급 및 평가시행은 국내 정보보호산업시장의 확대와 국가간에 CC 기반으로 평가·인증된 제품을 상호인정 해주는 국제공통평가기준 인정협정(CCRA, Common Criteria Recognition Arrangement) 가입과 연계된다.

〈표 2〉 보호프로파일 현황

보호프로파일 명칭	분류	평가등급	제/개정일
국가기관용 침입차단시스템 보호프로파일 V1.1	침입차단시스템	EAL3+	2003. 4. 30.
국가기관용 침입탐지시스템 보호프로파일 V1.1	침입탐지시스템	EAL3+	2003. 4. 30.
국가기관용 가상사설망 보호프로파일 V1.1	가상사설망	EAL3+	2003. 4. 30.
국가기관용 가상사설망 게이트웨이 보호프로파일 V1.1		EAL3+	2003. 4. 30.

〈표 3〉 CC 기반 평가 현황

연도	평가신청 수	평가등급	평가구분	평가완료일	비고
2003	2개 업체의 침입차단시스템과 가상사설망 통합제품 3건	EAL3+	최초	-	평가 중
		EAL3+	최초	-	평가 중
		EAL3+	최초	-	평가 중

〈표 4〉 CC 관련 국내 표준 현황

구분	표준번호	표준명	제/개정일
단체 표준	TTAE. CC-99. 031(CC-1v2.1)	국제공통평가기준-제1부 : 소개 및 일반모델	2001. 12
	TTAE. CC-99. 032(CC-2v2.1)	국제공통평가기준-제2부 : 보안 기능 요구사항	2001. 12
	TTAE. CC-99. 033(CC-3v2.1)	국제공통평가기준-제3부 : 보안 보증 요구사항	2001. 12
	TTAR-0011	보호프로파일 및 보안목표명세서 작성법	2002. 12

Ⅲ. CC 관련 국내 표준화 동향

국내의 단체 표준으로 제정된 CC 관련 표준에는 CC 버전 2.1의 1, 2, 3부 및 보호프로파일 및 보안목표명세서 작성법이 있으며〈표 4 참조〉, 이 밖에 CC 기반 정보보호시스템 평가의 효율성을 제고할 수 있는 형상관리와 생명주기 관련 표준안 등이 현재 개발 중에 있다.

Ⅳ. CC 관련 국제 표준화 동향

1. ISO/IEC JTC 1/SC 27의 소개

CC 관련 국제 표준화 조직으로는 ISO/IEC JTC 1/SC 27/WG 3이 있다. SC 27 회의는 ISO와 IEC의 공동기술위원회 (JTC 1) 산하의 정보기술 보안에 대한 국제표준 제정을 위한 국제회의로서 각국에서 임명한 정식 대표단이 모여 자국의 기술과 의견을 반영하는 회의이다. 한국은 산업자원부 기술표준원에서 국내 간사기관(National Body)을 담당하고 있고 SC 27 간사는 독일의 표준기관인 DIN(Deutsches Insititut for Normung)에서 맡고 있다.

ISO/IEC JTC 1/SC 27에서는 정보기술의 보안사항 중 보안메커니즘, 알고리즘, 평가방법, 보안서비스 등에 대한 표준화 작업을 담당한다. 그리고 표준은 IS(International Standard)와 TR(Technical Report) 등 2가지로 작업이 이루어지고 있으며, IS 바로 이전 단계를 DIS(Draft IS)라고 한다.

JTC 1/SC 27에는 3개의 WG(working group)이 운영되고 있으며〈그림 1 참조〉, 각 WG의 의장(Convener)은 다음과 같다.

WG 1(요구사항, 보안 서비스 및 지침) : Ted Humphreys(영국)

WG 2(보안기술 및 보안메커니즘) : Marijke De Soete(벨기에)

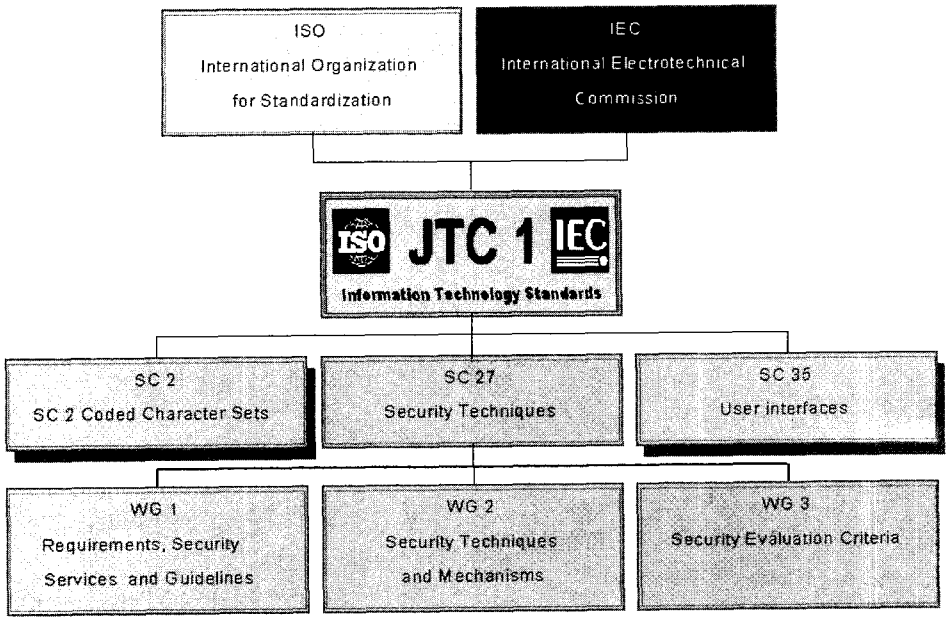
WG 3(보안성 평가) : Mats Ohlin(스웨덴)

2. WG 3의 표준화 동향

WG 3은 IT 시스템, 구성요소, 제품의 검증과 IT 보안 평가 표준, 컴퓨터 네트워크, 분산 시스템, 관련 응용 서비스 등을 포함하며 평가기준, 기준의 적용 방법론, 평가·검증·인증 스킴에 대한 관리상의 절차 등 3가지 측면을 취급한다.

지난 4월 28일부터 5월 2일까지 캐나다 퀘벡에서 열린 WG 회의는 우리나라와 미국, 영국, 독일, 일본 등을 포함한 12개국에서 총 20여 명이 참여하였으며 말레이시아, 남아프리카공화국의 2개국 대표도 참석하는 등 보안성 평가분야에 대한 국제적 관심이 증대되고 있다.

이번 WG 3에는 ISO/IEC PDTR 15443(IT 보안성 보증 프레임워크) 등 기존의 프로젝트와 국제표준 15408(CC) 유지관리 등에 관한 논의 이외에도 작년 10월 제 25차 폴란드 바르샤바 회의에서 제안된 신규 과제 3종을 프로젝트 19790(암호 모듈 보안 요구사항), 19791(시스템 운영 보안성 심사), 19792(생체인식 기술 보안성 평가·심사 프레임워크)로 하여 진행하기로 하는 등 신규 보안성 평가 표준화 중심으로 진행되고 있다〈표 5 참조〉. 다음은 신규 프로젝트에 관해 논의된 내용이다.



〈그림 1〉 ISO/IEC JTC 1/SC 27 체계

◦ 프로젝트 19790 : 암호모듈 보안 요구사항(Security Requirements for Cryptographic Modules) WG 2와 WG 3의 합동 미팅을 거쳐 신규 프로젝트 19790의 주 편집자로 미국 대표 Ms. Annabelle Lee, 공통 편집자로는 캐나다 대표 Mr. Mike Chawrun, 프랑스 대표 Mr. Jean-Pierre Quemard가 임명되었으며, 미국, 캐나다, 영국 등에서 현재 사용되고 있는 미국 표준 FIPS 140-2의 컴퓨터 및 통신시스템암호 모듈 보안요구사항에 대한 소개가 있었다. 진행 방향에 대한 논의로는 본 프로젝트의 기반인 FIPS 140-2는 여러 참조 문서 중 하나로만 활용되어야 하며 IS 15408, DIS 18045 등도 참조되어야 한다는 독일의 안과 IS 15408을 중심으로 진행되어야 한다는 스페인 안 등이 제기되었다.

미국 대표 Ms. Annabelle Lee가 WG 2, 3 합동 미팅에서 소개한 프로젝트 19790의 범위에는 FIPS 140-2의 암호모듈 명세, 암호모듈 포트 및 인터페이스, 서비스 및 인증, 암호 키 관리, 자체-시험, 설계 보증 등이 포함되며, 향후 진행 일정으로 WG 3 의장은 미국 대표에게 2003년 7월 1일까지 WG 2, 3 합동 미팅에서 논의된 내용을 반영한 첫 번째 WD(Working Draft)를 SC 27 사무국에 제출할 것을 요구하였다.

◦ 프로젝트 19791 : 시스템 운영 보안성 심사(Security Assessment of Operational Systems) 이번 WG 3에서 본 프로젝트의 편집자로 일본 대표 Mr. Haruki Tabuchi가 임명되었다. 본 프로젝트에 대하여 WG 3은 IT 시스템 보안성 평가기준으로 제정된 ISO/IEC 15408(CC)을 기술 메커니즘과 운영관리 측면이 통합된 시스템 평가에 적용하기 위한 시스템 평가 프레임워크 필요성을 제기하였으며, 프로젝트가 진행되면서 다양한 물리적 논리적 세그먼트로 구성된 시스템 TOE에서의 도메인 정의 문제 해결방법과 시스템 평가방법에 대해 논의하였다.

이 밖에 제품 평가에 초점을 맞추고 있는 ISO/IEC 15408(CC) 보안요구사항과 평가보증등급 패키지에 인적, 운영측면을 보강한 새로운 보안요구사항 및 평가보증등급 패키지를 만들자는 일본의 안(예 : Personnel security를 위한 PPS 보안기능요구사항 클래스, Security awareness를 위한 ASA 보증요구사항)과 기존의 패키지로 단순한 시스템부터 복잡한 시스템까지 적용이 가

〈표 5〉 ISO/IEC JTC 1/SC 27/WG 3의 표준화 현황

표준 번호	표준과제명
ISO/IEC 15408-1 : 1999	part1 : introduction and general model
ISO/IEC 15408-2 : 1999	part2 : Security functional requirements
ISO/IEC 15408-3 : 1999	part3 : Security assurance requirements
ISO/IEC 15292 : 2001	Protection Profile registration procedures
ISO/IEC PDTR 15443-1 : 2003	part1 : Overview and framework
ISO/IEC PDTR 15443-2 : 2003	part2 : Assurance methods
ISO/IEC WD 15443-3 : 2001	part3 : Analysis of assurance methods
ISO/IEC PDTR 15446 : 2001	Guide on the production of Protection Profile and Security Targets
ISO/IEC WD 18045 : 2002	Methodology for IT security evaluation
New Project 19790 : 2003	Security Requirements for Cryptographic Modules
New Project 19791 : 2003	Security Assessment of Operational Systems
New Project 19792 : 2003	A Framework for Security Evaluation and Testing of Biometric Technology

능하다는 독일의 안 등이 논의되었다.

향후 일정으로는 일본 대표 Mr. Haruki Tabuchi에게 프로젝트 19791의 원활한 진행을 위하여 2003년 7월 10일까지 N3516, N3527, N3534의 내용을 반영한 첫 번째 WD(Working Draft)를 SC 27 사무국에 제출할 것을 요구하였다.

◦ 프로젝트 19792 : 생체인식 기술 보안성 평가 시험 프레임워크(A Framework for Security Evaluation and Testing of Biometric Technology) 본 프로젝트의 편집자로 ArsLan Bomme가 임명되었으며, 생체인식 보안성 평가에 대한 프레임워크에 대한 프로젝트 19792의 내용 소개보다는 향후 본 과제의 진행 방향과 범위에 대한 논의(SC 37과의 범위 중복)가 있었다. 향후 일정으로는 프로젝트 19792에 대한 다른 국가의 조언을 2003년 10월 1일까지 받기로 하였다.

V. 맺음말

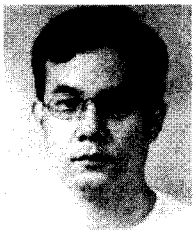
본 고를 통해 우리나라의 정보보호시스템 보안성 검증을 위하여 활용되고 있는 CC의 국내 현황과 국내 표준화 기관 및 ISO/IEC JTC 1/SC 27에서 진행되고 있는 국내·외 표준화 동향에 관해 살펴보았다. 우리나라는 2002년에 고시한 정보보호시스템 평가 인증지침에 의거 CC 기반 보호프로파일 개발 및 정보보호시스템 평가를 시행 중에 있으며, 다양한 제품군으로 확대해 나가고 있다. 또한 CC와 연계된 ISO/IEC JTC 1/SC 27의 표준을 국내 실정에 맞게 수용하는 등의 노력을 관계기관과 협력하여 진행하고 있다. 이는 우리나라가 목표로 하고 있는 국제공통평가기준 인정협정(CCRA) 가입 과정 중 중요한 부분을 차지한다고 판단된다. 향후에도 우리나라는 산·학·연 관계기관의 협력을 통해 CC 기반 평가역량확충 제고 및 미개발 표준화 과제의 발굴·표준화를 추진함으로써 평가부분의 국제적 입지를 더욱 더 확대해 나가야 한다고 사려된다.

참 고 문 헌

〔1〕 정보보호시스템 평가 인증 가이드, 한국정보보호진흥원, 2002. 12.

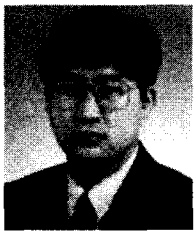
〔2〕 정보통신부고시 제2002-41호, 정보보호시스템 평가 인증 지침, 2002. 8.
〔3〕 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5.
〔4〕 Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, http://www.commoncriteria.org, 2000. 5.
〔5〕 HTTP://www.din.de/ni/sc27
〔6〕 ISO/IEC JTC 1/SC 27 N3591 "Draft SC 27/WG 3 Resolutions-Meeting Number 26 28th April-2nd May 2003 Quebec, Canada", 2003. 5. 2.
〔7〕 ISO/IEC JTC 1/SC 27 N3466 Revised summary of voting on NP 19790 "Security requirements for cryptographic modules", 2003. 2. 21.
〔8〕 ISO/IEC JTC 1/SC 27 N3527 NP 19791 "Security Assessment of Operational Systems", 2003. 4. 9.
〔9〕 ISO/IEC JTC 1/SC 27 N3468 Revised summary of voting on NP 19792 "A framework for security evaluation and testing of biometric technology", 2003. 2. 21.
〔10〕 ISO/IEC JTC 1/SC 27 N3516 "SC 27 Liaison Statement to SC37", 2003. 5. 2.

저 자 소 개



이 태 승

1994년 2월 광운대학교 전자계산학과(이학사), 1996년 2월 포항공과대학교 전자계산학과(공학석사), 1996년 2월~2002년 1월 : 삼성전자 소프트웨어센터, 2002년 1월~현재 : 한국정보보호진흥원 평가기준팀, 〈주관심 분야 : 정보보증, 무선인터넷 보안, 전자지불보안〉



노 병 규

1988년 2월 충남대학교 계산통계학과(이학사), 1995년 2월 충남대학교 계산통계학과(이학석사), 2003년 12월 순천향대학교 전자계산학과 박사수료, 1988년 2월~1997년 2월 : 한국전자통신연구소, 1997년 1월~현재 : 한국정보보호진흥원 평가기준팀, 〈주관심 분야 : 정보보증, 네트워크 보안, 시스템 보안〉